科技情报中的信息安全思考

高美玲[1]， 赵淦森[1,一]

[1]华南师范大学图书馆 广州 510631

[目的/意义]科技创新所形成科技情报是我国科技创新活动的重要成果，科技情报的信息安全深刻地影响着我国的科技安全与国家繁荣昌盛。研究科技情报的信息安全问题，既有利于主动发现科技情报中的安全漏洞，提前研判安全风险和处置安全漏洞，避免安全问题发生；也有利于建立科技情报安全工作机制和技术保障体系，提升国家科技情报信息安全，保障国家的科技创新安全。**[方法/过程]**从科技情报的信息安全分析入手，剖析科技情报的信息安全内涵、挖掘存在的信息安全问题及潜在的安全风险，总结导致信息安全问题的原因；开展科技情报的信息安全保护策略分析，提出科技情报的信息安全保护建议，探索应对科技情报信息安全问题的对策。**[结果/结论]**科技情报安全问题总结归纳为信息泄露问题、数据破坏问题和定向研究误导问题。保护科技情报的信息安全过程中存在无感知、难预防、难监控、难取证、难甄别和难应对等挑战。保护科技情报的信息安全建议从科技情报分类分级、设施保护、数据保护、权限保护和信息安全技术应用五个层面同步开展。同时，加强科研人员的科技情报保护意识，加大应对科技情报网络攻击的监测，以及研发推广应用于科技情报的数字指纹等技术对于保护我国科技创新的安全至关重要。

关键词：科技创新 信息安全 科技情报安全

分类号：G351.1

我国经济社会持续快速发展，科学研究和技术创新取得长足进步，创新能力不断提升，科技创新在经济社会发展中的作用越来越突出。科技创新成为大国竞争的主战场，国家科技创新关系到世界大国之间的竞争和博弈，而维护科技创新的安全对保障国家总体安全意义重大。近年来，由于科技创新的安全问题，科技创新竞争所导致的贸易摩擦频出不穷，部分高端产业惨遭外国“卡脖子”，对我国产业和国家安全构成严重威胁。随着国际政治局势的风云变幻与大国竞争的冲突升级，科技创新的安全被世界主要国家和地区视为影响国家安全的新因素。研究科技情报的信息安全问题，对于保障我国科技创新安全意义重大。一方面，可发现科技情报中的安全漏洞并研判安全风险，做好提前处置工作，避免出现科技情报安全事故。另外一方面，通过科技情报安全研究建立科技情报安全工作机制，健全科技情报的应对措施，保障国家科技创新安全。

本文的研究思路如图 1 所示，以科技情报安全研究动机、科技情报内涵、原因剖析、挑战分析、应对策略和建议作为研究的主线。首先从研究科技情报信息安全的意义出发，鉴别科技情报信息安全的内涵，分析科技情报信息安全保护中存在的问题，剖析导致信息安全问题的原因。其次，分析了科技情报信息安全保护工作存在的诸多挑战，并基于保护科技情报信息安全的挑战设计了相应的保护策略，并针对性地提出面向科技情报信息安全保护的建议。

一 通讯作者, gzhao@m.scnu.edu.cn.

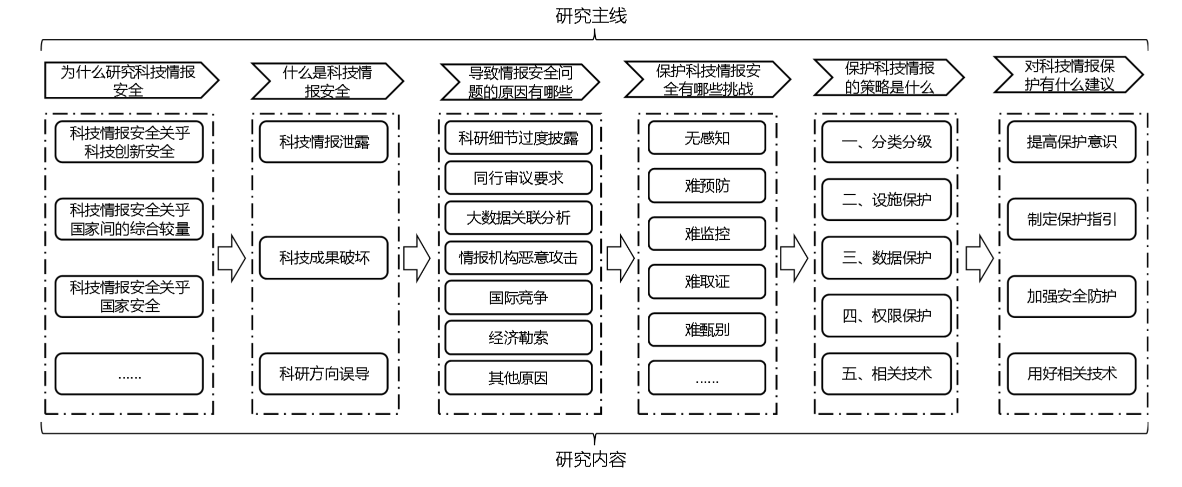


图 1 本文的总体研究思路和研究内容

本文的研究贡献主要包括三个层面。首先，阐述了科技情报安全保护的重要性，倡导更多科技创新研究人员关注科技创新工作中的情报安全问题。其次，系统性地分析了科技创新工作中的情报安全问题，识别出科技创新工作中容易导致出现情报安全问题的风险点，并给出保护科技情报安全的相关策略和建议，为提前谋划科技情报安全保护措施，避免出现科技情报事故提供了重要参考。最后，本文提出科技情报的信息安全的思考，以此作为引子，抛砖引玉，倡导更多研究者共同加入科技情报安全的研究工作，共同守护国家科技创新安全。

1 科技情报的信息安全问题分析

1.1 科技情报信息安全内涵

科技创新成果是科学研究和技术创新所产生的成果。科技创新成果伴随智力创作和经营活动产生，是一种重要的高价值无形资产，具有推动科技发展和促进经济增长的重要作用[1]。由于科技创新成果的高价值和排他特性，被许多企业用作为筑建企业经营核心竞争力的重要工具和手段，甚至被许多国家用于大国之间竞争的重要抓手[2]。

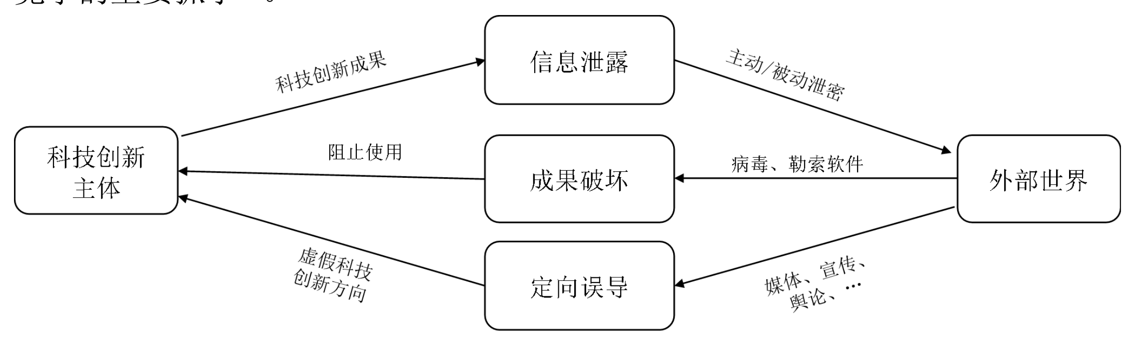


图 2 科技情报安全的内涵

由于科技创新所形成的科技情报对于国家安全与企业核心竞争力等方面的重要性，科技情报一直是信息安全问题高发的领域[3]。科技情报的信息安全问题，如图 2 所示，包含三个层面的含义：一个是科技创新主体在开展科技创新活动中所取得的科技成果通过主动或者被动的方式泄露到科技创新主体之外的外部世界，导致科技创新成果的查看、传播不受主体控制，进而造成科技情报的泄露；二是外部世界通过病毒、勒索软件等方式，对我国科技创新成果进行破坏，导致科技创新主体无法正常使用已有的科技创新成果；三是外部世界通过主导的媒体、

宣传、舆论、研究报告等方式有意或者无意传播定向误导的科技情报内容，扰乱我国科技创新主体的研究思路和研究方向，干扰我国科技创新的进展。

1.2 科技情报中的信息安全问题

科技创新是第一生产力，是促进国民经济增长，保持社会稳定，保障国家安全的重要力量，也是国际竞争的重要较量领域。科技创新中的信息安全事件关乎社会稳定和国家安全，图 3 汇总了千禧年之后引起国际社会重点关注或后果及其严重的信息安全事件。

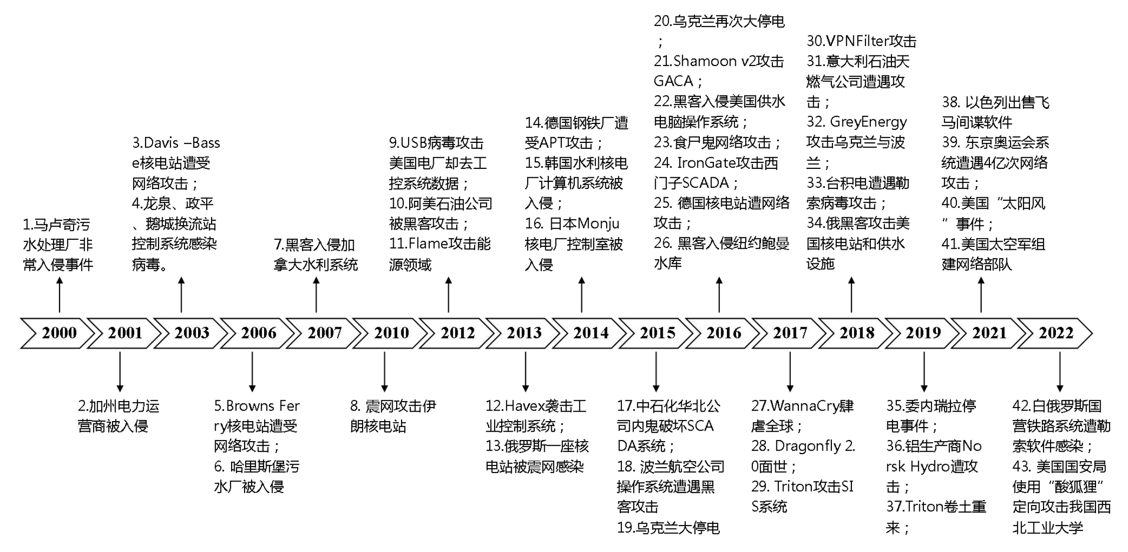


图 3 涉及国家安全的重大信息安全事件汇总

在科技创新领域中，我国成为全球网络攻击的主要受害国。在我国的科技创新和科技攻关历程中，多个以国家为背景的攻击组织，针对我国网络攻击的活动从未间断，给我国的信息安全带来严重的挑战[4,5]。2020 年，正当我国众志成城抗击新冠疫情之际，360 安全大脑捕获美国中央情报中心（CIA）的网络攻击组织（APT-C-39）仍在对我国开展大规模的网络渗透攻击[6]。海莲花（Ocean Lotus）、响尾蛇（Side Winder）、奇幻熊（APT28）、蔓灵花（Bitter）、白象（Hang Over）和寄生兽（Dark Hotel）等重大科技情报的信息安全事件，严重影响了我国科技创新工作的进程[7]。

云计算、大数据、人工智能、区块链和 5G 通信等新兴技术的兴起，支撑各科研院所建立了超大规模的科技情报信息检索中心（如各高校线上图书情报中心），同时也成就了有偿面向个人和机构开放的科技创新成果运营平台（例如知网、万方、维普等）。科技创新成果的电子化和数字化，致使科技情报采集、传播和使用的可控范围发生了巨大变化，导致科技情报的安全面临诸多风险和挑战。罗骄等学者从管理层面将科技情报中的安全管理问题总结为三个方面，分别为产权缺位问题、主权缺失问题和共享受阻问题[8]。区别于现有研究成果，本文则重点从信息安全的技术角度，对科技情报的安全问题进行总结，并归为三大类：科技情报的信息泄露、科技创新成果的数据破坏和科技情报的定向误导。

1.2.1 信息泄露

科技情报的信息泄露问题是科技创新的保护成果突破了既定的数据访问边界，流转到非授权访问人员或者机构中，导致科技创新成果数据被不当访问。科技情报的信息泄露存在许多种可能路径，例如黑客攻击、物理设备销毁不当、账号密码管理不善、内部人员主动泄露等。信息泄露是科技情报信息安全中最常见

的问题之一。科技情报的信息泄露主要包括三种类型：主动泄密、过失泄密和被动泄密。

（1） **科技情报的主动泄密**

部分被境外势力策反的内部科技创新工作者以学术交流等幌子主动泄露我国科技情报信息。主动泄露科技情报的行为人往往是科研创新的内部研究人员，其主观恶意性大，其行为具有高度的隐蔽性，其后果对国家科技创新安全带来严重危害。

行为人在科技文献写作中，超出学术交流程度对外披露科技创新的研究动机、工作意图、技术路线、业务应用场景、工作进展、核心参与工作者以及引用涉密文献等核心情报信息，导致重大科技创新情报信息泄露。例如，行为人在科技文献写作中，故意违反科技创新安全保护工作规定，通过脚注和参考文献等方式引用涉密代码或者涉密文件名称，导致国家科技创新机密泄露；或者在文献的工作意图中详细描述当前研究所要解决的具体“卡脖子”问题，在研究进展中描述当前不宜公开的研究进展细节，泄露获得研究成果的具体方法等相关内容，导致竞争者对相关研究快速跟进或者加大技术封锁。

部分科技情报泄露者为逃避科技情报安全监管，使用事先约定的加密方式将科技创新的核心研究成果内容加密后编码到图像或者视频等非结构文件中，并通过学术交流、社交媒体等看似“正常”的活动对外泄露。例如通过将单通道的灰度图像使用三通道格式进行保存和传输，并在多余的两个通道使用事先约定的加密方式藏匿核心情报内容，使得在不改变灰度图像正常显示的基础上，使用携带已加密核心情报信息的灰度图像对外泄露情报信息。

（2） **科技情报的过失泄密**

科技情报的过失泄密是科技创新工作者在日常的对外交流或者学术研讨中，出于工作疏忽或者个人保护意识不足，将科研创新中所取得的关键性研究进展等不适宜公开的情报信息对外公开。科技情报创新的过失泄露，其行为主管恶意性相对较低，但其所导致后果的严重性并不一定会低。

科技情报的过失性泄露主要表现为行为人对于所参与的科技创新工作的背景缺乏认知，科技情报的保护意识不足，通过在社交平台、面对面聊天、学术论坛或者学术写作等方式中不恰当地描述了所开展工作的具体内容细节，例如所参与相关科技创新的细节、合作机构、合作人员分工、某个关键研究内容的具体研究进展、研究所提出的核心方法等相关内容，导致情报信息的泄露。又例如，行为人在社交媒体发表相关动态时拍摄了看似与工作无关的相关照片，通过照片的元信息泄露照片的拍摄时间、拍摄经纬度、拍摄设备等相关基础信息，从而无意泄露行为人的所科研机构的相关信息。

（3） **科技情报的被动泄密**

科技创新成果通过科技文献、学术论坛、专利、新闻等方式有条件地对外进行公开和交流。大数据技术可以通过收集分散的科技创新研究成果、文献引用和被引用关系等分散信息，开展科技情报的精准挖掘、关联分析和知识图谱等聚合性分析，构建基于时间轴的研究合作者关系、研究兴趣、研究方向、研究进展预测等科技创新成果挖掘模型，从而将零散的科技创新成果素材加工成体系化的科技情报[9]。通过使用大数据对分散科技成果的关联分析，聚合形成完整的科技研究动态进展视图，从而反映了特定领域科研创新攻关工作的研究布局、研究进展、研究拓扑关系等核心情报信息，从而造成核心科技情报的被动泄露。

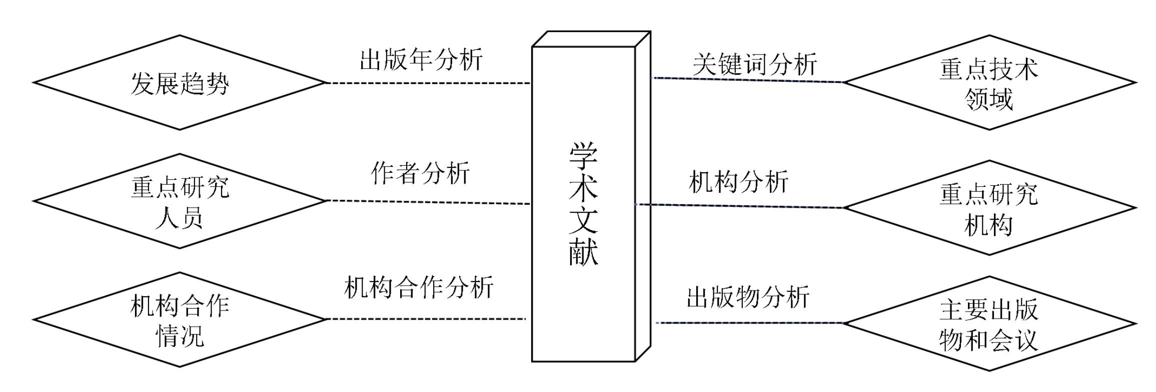


图 4 大数据关联分析致使情报泄露流程示例

基于大数据关联分析的科技情报泄露过程如下，基于数据库中收集的学术文献，对其出版时间、作者、发文机构、机构合作、资助基金、关键词以及出版物等相关要素开展聚合分析，形成特定地区在信息安全领域学术研究的发展趋势、重要研究人员、重要研究机构、机构合作情况、基金资助机构、重要技术领域以及该研究涉及的主要出版物和学术会议，并在此基础上，选取发文量较多的重要研究人员、重点科研机构和重要学术会议进行重点分析。图 4 展示了大数据关联分析导致科技情报泄露的流程示例。

1.2.2 数据破坏

科技创新成果数据被病毒和勒索软件等方式恶意破坏，导致科技创新成果无法继续使用是科技创新中遇到的最常见的信息安全问题之一。科技情报的数据破坏是指科技情报数据的一致性、完整性和可用性遭到意外破坏，使得系统保存的数据不能客观反映科技创新成果的客观事实，导致科研、经济活动无法使用或者错误使用“数据失真”的科技成果，也有可能导致科技创新主体无法辨识或者证明该科技创新成果的真伪性、隶属关系等相关属性，并最终影响科技创新成果的实际科研和经济价值。常见通过破坏数据实现科技创新信息安全攻击的方式包括蠕虫攻击、木马攻击、数据加密和数据删除等方式[10]。

1.2.3 定向误导

对科技创新的信息安全攻击，除了获取目标机构的科技创新成果进展和破坏对方科技创新活动之外，还包括诱导目标机构开展错误的科技创新研究，使其误入歧途。例如，某国外著名学者通过伪造数据的方式，在著名期刊发表“淀粉样蛋白假说”的“开创性”研究论文[11]，使其成为阿尔兹海默症等多种神经疾病的发病机制假说，该研究自公开发表以来，引用频次超过 2300 次，通过虚假研究的方式误导大量科技创新团队的研究方向[12]。

1.3 科技情报的信息安全问题原因探索

引起科技情报信息安全问题的原因有很多，本文分别从科技情报信息泄露、科技创新数据破坏和科技情报定向误导三个层面展开分析和总结。

1.3.1 科技情报信息泄露原因分析

导致科技情报信息泄露的原因总结起来主要包括科技创新学术交流细节的过度披露、科技创新成果同行审议要求、大数据关联分析、情报机构的恶意攻击与信息收集等原因。

（1） 科技创新成果细节过度披露

学术研究论文是科技创新成果对外交流的重要载体。在科研论文的写作过程中，研究人员在论文中阐述论文的研究动机、工作意图、所设计的整体技术路线、适用的业务场景、开展科技创新的组织机构、参与科技创新的核心人员、科技创

新成果的进展、未来的重要研究展望及研究计划等相关科技创新内容。这些内容一方面向读者概述了科技创新研究的研究背景、方法所取得的成效，但另外一方面对于细节的过度披露则一定程度上导致了该科技创新成果的核心情报信息泄露。竞争对手或者外部势力通过对我国核心领域的研究论文的深入分析，实现对我国科技创新情报的刺探，一定程度上还原出相关的科技创新的内容细节。

除此之外，研究人员在开展涉密科技创新工作过程中，对于尚未脱敏的科技创新成果进行公开发表，是导致科技情报泄露的其中一个直接原因。例如，国内多个知名数据库网站同时刊登 1 篇涉及国家科技创新秘密的研究论文。后经组织相关专家进行鉴定，该论文所描述内容属于秘密级的国家秘密。经过深入的调查，该论文作者受到在某涉密工作单位亲属的协助请求，协助完成该涉密科技创新的某个具体算法后，私下复制、保存相关内容，且在未经过专业脱敏操作后，直接撰写成科研论文对外公开发表，导致某涉密机构的科技创新秘密被不当泄露，对我国科技创新安全和科技情报安全带来严重威胁[13]。

（2） 科技创新同行审议要求

在科技创新成果的发表过程中，大量期刊要求科研人员投稿时需要提供可复现的相关算法、实验材料清单或者数据集等详细的过程材料，以方便同行审稿专家对科技创新成果的复现和判定，以决定是否录用该科技创新成果，并在录用后对外公开，以供读者下载。对于科技创新成果而言，研究所获得的结论固然重要，但是支撑研究的所有过程细节、材料、算法等内容也属于科技情报的保护范畴。研究人员为提高科技创新成果被期刊审稿专家的认可度和投稿接收率，超出期刊同行审议的要求，上传相关的数据、算法细节等行为，一定程度上加大了我国科技创新成果的安全风险，轻则导致我国重要的科技情报泄露，重则危害国家科技创新安全。近期，国家出台禁止生物数据出境条例[1]，反映了科技创新成果的核心数据出境不仅损害国家科技创新安全，造成重要的科技情报泄露，危害国家安全。

（3） 大数据关联分析

大数据的关联分析是一把双刃剑。科技情报刺探人员通过在公开网站（例如谷歌学术、知网）针对某一科技创新主题或者某一科技创新主体，开展科技创新所形成的论文、专利等成果的收集工作，利用大数据分析技术构建科技情报知识图谱，从而分析某个国家、某个实体或者某位研究人员的科技创新研究进展、研究成果、开展科技创新的研究人员与研究机构的关系图谱等，挖掘出相关科技创新的情报价值，并用于支撑制定企业竞争和大国较量策略。当前，大数据技术被广泛地应用于科技情报的分析工作，通过大数据分析技术构建科技情报关系图谱，极大地降低了科技创新成果数据分析的难度，提高了科技情报收集和刺探的效率，增大了保护科技情报信息安全的难度。

（4） 情报机构的恶意攻击与信息收集

情报机构通过网络攻击或者社会工程攻击等方式，进入到目标科技创新情报的非授权区域，通过窃取或者渗透等方式获取组织机构内部的科技情报机密材料、尚未发表或者尚未脱密的科技创新技术材料，从而导致组织机构科技创新成果的泄露。情报机构通过策反内部人员主动对外发送科技创新的核心成果情报或者国家机密的社会工程攻击往往难以察觉，一旦发现已经造成了重大严重后果。例如，社科院原职工某博士遭到境外情报机构的策反，将国家核心机密、知识产权等重

[1] 工业和信息化领域数据安全管理办法（试行）（征求意见稿）、《生物安全法》

要的科技创新成果和情报通过论文的方式输出多个境外国家，对我国的科技安全、国家安全造成重大危害[10]。

1.3.2 科技创新数据破坏原因分析

要剖析科技创新成果数据破坏的原因，就需要先分析实施数据破坏行为的主体。面向科技创新成果实施数据破坏的主体主要包括三大类，分别是政府组织背景的机构、民间黑客组织以及单兵黑客。政府组织机背景的机构对他国开展科技创新成果破坏的主要原因和出发点是包括但不限于政治、军事、经济等因素在内的国家利益驱动。民间黑客组织发起科技成果数据破坏的主要原因出于类似赎金解密等经济诉求，同时也存在政治站队原因。例如俄乌战争期间，InvisiMole、Vermin 和 APT-28 等著名黑客组织由于抗议相关方频繁发动俄罗斯或乌克兰网络攻击[14]。单兵黑客发起对科技创新成果的数据破坏主要出于三类目的和原因，分别是经济诉求、个人政治站位和攻防技术演练等原因。

1.3.3 科技情报定向误导原因分析

引起定向科技情报误导的原因包括政治原因和个人原因。其中，政治原因是某些研究机构和主体，受到某些特定单位的资助后为配合当局开展治理工作，根据指向性结论设计研究过程、研究方法、定向收集研究数据，从而推理出既定的研究结论。其次，在科技情报的定向误导中，受到个人职业生涯发展等现实困境所需科技创新业绩的要求，通过数据作假和实验作假等方式，撰写虚假结论的科技创新文献并对外公开发表。

2 面向科技情报的信息安全保护挑战

保护科技创新和科技情报的信息安全，面临诸多的挑战[10, 15, 16]。根据对科技创新和科技情报信息安全问题的原因分析，本文分别从避免科技情报信息泄露、防止科技创新成果数据被恶意破坏以及避免科技创新被定向误导三个维度进行分析。

2.1 避免科技情报信息泄露的挑战

科技情报的信息安全保护工作存在诸多挑战，可以总结为“无感知、难预防、难监控、难取证和难甄别”。

（1） 无感知

科技情报面临信息安全问题时，科技创新主体难以感知正在面临的信息安全风险。由于缺乏面向科技情报安全监测和感知的统一支撑平台，当科技情报正在面临信息安全风险时，科技创新机构难以第一时间感知到“危险”的存在，甚至在“事后”仍然难以觉察到科技创新成果已经遭受了“侵害”。

（2） 难预防

情报机构对科技创新成果开展攻击时，综合分析科技创新成果的保护状态，进而采取不同的攻击手段，从而获取到对应的科技情报。其中攻击的方法包括但不限于 DDOS 攻击、木马病毒攻击以及社会工程攻击等手段。同时，攻击者对相关科技创新成果的攻击具有标的不确定性、时间不确定性和手段不确定性。因此，对于科技创新成果等科技情报的信息安全保护，具有“难预防”的挑战。

（3） 难监控

科技创新工作由不同的科研机构和科技研究者承担，所研究获得的科技成果具有存储分散、主体分散、形式多样的特点，导致科技情报泄露具有源头分散、主体分散、时间分散和形式分散的特性。因此，难以针对科技情报信息泄露进行有效地监控。

（4） 难取证

由于可能导致信息安全泄露的源头众多，且大量的科技创新成果缺乏使用数据指纹等标识技术对内容进行唯一化标识，难以溯源已发生泄露内容的泄露路径，对于造成严重损失或者后果的科技情报信息安全事件，难以开展科技情报信息泄露的审计取证工作。

（5） **难甄别**

在科技情报防泄漏保护工作中，一方面科技创新组织难以甄别组织内部成员是否已经遭受社会工程攻击而成为科技创新成果主动泄露人员。另外一方面，科技创新工作中难以甄别可能会导致信息泄露的设施和对应环节。科技创新成果的撰写和成果交流中，难以权衡对外披露信息的详细程度，难以甄别导致科技创新信息泄露的临界点。

2.2 避免科技创新数据被破坏的挑战

对攻击发起侧分析可知，科技创新主体难以预料和控制针对科技创新成果和科技情报开展攻击的组织或攻击者的行为。从攻击手段分析，科技创新主体难以有效且及时地应对日益改进的攻击工具和攻击手段。从科技创新成果和科技情报的保护层面分析，难以有效地针对数以千万计的科技创新组织和个体所获得的研究成果实施有效的保护策略或者升级相应的防护策略。

2.3 避免科技创新被定向误导的挑战

在科技创新工作中，大量的科技创新成果通过学术研究期刊、学会会议、专题研讨会和技术博客等途径对外公开。对于不同科技创新成果所陈述内容的真伪一方面需要大量的专业知识和对前沿研究的把握进行综合判断，另外一方面，对于科研创新“无人区”的开创性研究，需要通过后续大量新的研究对其进行验证。因此，避免科技创新被定向误导不仅存在着主观能力的挑战，同时也存在客观现实上的困难。

3 面向科技情报的信息安全对策探索

科技情报的信息安全保护是一个体系化的工作[1, 15, 17, 18]，需要对科技创新成果的产生、存储、传播和使用环节所涉及的基础设施、网络、软件和管理进行综合性分析，从而制定相关的安全保护对策。

3.1 面向科技情报的信息安全保护策略分析

本文提出面向科技情报的信息安全保护策略，如图 5 所示。分别从科技情报分类分级体系、设施保护、数据保护、权限保护和信息安全保护技术五个维度构建科技情报的信息安全保护策略。

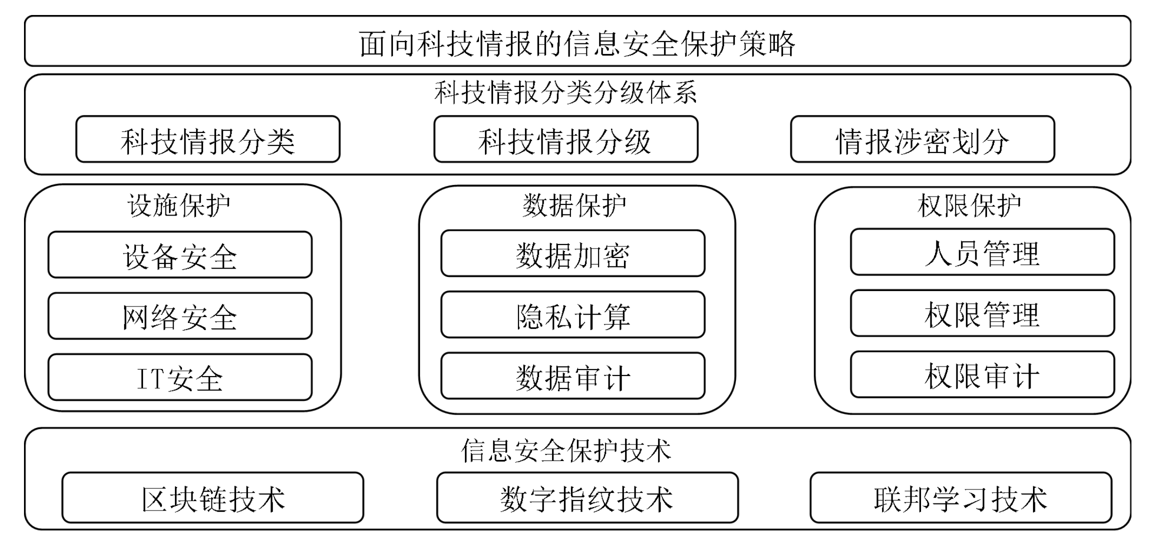


图 5 科技情报信息安全保护策略框架示意图

（1） 科技情报分类分级体系

科技创新所研究内容及其获得成果的重要性是无法一概而论的，同时科技创新所带来的情报价值的密度和可忍受的保护成本也存在天壤之别。受美国数据分类分级工作的启示[19]，面向科技情报的信息安全保护工作需要建立有效的科技情报分类分级体系，根据科技创新的研究内容、使用用途等进行分类，依据科技创新成果遭受信息安全攻击后所带来的损失、对我国科技创新的发展、产业发展和国家安全等涉密维度的影响程度进行分级。依据科技情报分类分级体系，以类别和级别制定科技情报保护的规范体系和保护措施要求。

（2） 科技创新设施保护

面向科技创新设施的保护主要目的是防止硬件设施的后门导致科技创新成果等科技情报数据的损坏、丢失或者泄露。其保护的对象包括服务科技创新工作的设备、核心的网络以及其他 IT 配套设施，尽最大可能地减少服务科技创新的设施出现数据泄露、数据破坏、数据丢失等损害科技创新的事件发生。例如逐步采用信创硬件设施逐步替换现有核心环节的设备，逐步消除现有基础设施国外设备后门泄露的风险。

（3） 科技情报数据保护

科技情报数据保护的主要目的是在保护科技创新成果等核心情报的情况下进行有条件的分享传播，同时避免科技创新成果的数据遭到恶意破坏。数据保护策略主要围绕科技创新成果等情报数据的加密、隐私分析和审计等角度开展科技情报数据的保护工作。例如，通过使用同态加密技术对科技情报数据进行加密操作，使用可证明数据持有模型（Provable Data Possession, PDP）和可恢复模型（Proof of Retrievability, PoR）对科技情报数据进行审计。

（4） 科技创新组织权限保护

科技创新组织权限保护的目标在于做好科技情报的访问、传播和边界控制，防止科技创新成果及其所形成的科技情报被泄露。科技创新组织的权限保护围绕涉及开展科技创新的机构、人员、访问权限和审计权限管理等工作。例如通过融合基于角色访问控制（Role-based Access Control，RBAC）、基于属性访问控制技术（Attribute-based Access Control，ABAC）和生物识别认证等方式，实现对科技创新核心成果访问权限的细粒度管理。

（5） 信息安全保护技术

为实现信息安全保护策略，建议底层使用区块链技术[20]对科技创新成果等情报数据进行分布式记录，保障科技创新成果数据的全链条可溯源，防止科技创新成果数据被篡改；其次采用数字指纹技术[21]对科技创新成果数据进行编码，确保同一份数据在不同用户、不同终端、不同时间的指纹信息具有唯一性，从而支撑科技情报的审计工作；采用联邦学习技术[22]对科技创新成果数据开展分析工作，使得研究人员能够实现在保护科技创新成果的前提下挖掘科技情报数据的价值。例如使用隐私规则

3.2 面向科技情报的信息安全保护建议

本文从提高科技创新主体的情报数据保护意识、保护机制、安全防护和数字指纹技术等方面提出面向科技情报信息安全保护的建议。

（1）科技创新主体单位提高科技情报保护意识

科技创新主体单位和个人是科技情报产生的主体，也是保护我国科技情报安全，避免被不当使用和传播的第一责任主体。加强对科技创新主体单位和个人的安全培训工作，提高科技创新主体的情报安全保护意识，能够有效地降低科技情报泄露的风险。科技情报的信息安全保护的第一责任主体是信息安全的权属机构。科技创新成果拥有单位和创造主体需要重视科技情报的安全对于国家安全和经济发展的重要性，树立科技情报的保护意识，严防科技情报出口关。

（2）主管机构加快制定科技创新成果保护指引

为保障我国科技创新成果能够高效赋能科技进步、产业发展和学术交流等工作，服务国家经济发展和民族创新，同时确保我国科技情报的安全，建议主管机构加快完善科技创新成果的保护政策和指引，研究制定涉及国家安全和“卡脖子”的科技创新成果保护指引，引导科技创新主体加强核心成果保护和防范信息泄露保护指引。根据科技创新成果的重要程度、经济价值、服务国家安全等相关因素，开展科技创新成果分类、分级工作，并对不同类别和级别的科技创新成果采取不同的保护等级和措施，确保国家科技创新安全。

（3）科技创新服务平台加强系统安全防护

科技创新服务平台一方面充当了科技创新服务经济社会，促进技术交流的重要角色，另外一方面的也充当了科技创新成果汇聚和集中存储的重要角色。科技创新服务平台中存储了我国大量科技创新成果，是重要的科技情报中心，一旦发生信息泄露，将对我国的科技创新和国家安全带来极大风险。为此，建议科技创新服务平台加强网络安全防护工作，及时排查和封堵网络安全漏洞，提高平台抗击网络攻击能力，避免由于平台漏洞导致我国科技创新成果面临泄露风险。

（4）加快研发和推广数字指纹技术

科技创新成果大多以电子档案为载体进行存储、传输、编辑和查阅。电子文档的可无限复制特性让科技情报在发生不当传播后难以对泄露内容进行溯源，不利于事后分析科技情报的泄露源头。因此，建议基于区块链、数字指纹等技术加快研发面向科技情报保护相关应用，基于数字指纹技术对科技创新成果进行登记、查阅和传播，促进科技创新成果的全过程可查阅、可溯源、可审计，识别科技情报泄露源头，加大打击科技情报泄露力度。

4 结语

当前，受到全球新冠疫情大流行、经济下行和地区摩擦不断等不稳定因素影响，世界秩序正在经历百年未有之大洗牌阶段。中西竞争竞争愈演愈烈，贸易摩擦不断，我国科技创新和产业发展频遭外国技术封锁，国家自主科技创新安全事

件频发[23]。当前，国家正处于不同领域开展具有自主知识产权的科技创新攻关研究的关键阶段，力求通过科技创新不断地突破西方先进技术对国家科技创新的技术封锁、产业发展和国家安全的限制。

国家科技创新的情报安全不仅关乎国家前途命脉和民族复兴，同时也关乎世界大国竞争的格局变化。保护国家科技创新的情报安全就是保护国家科研创新的安全、也是保护国家产业的安全，更是保护国家战略的安全。本文以科技创新安全研究的重要性、内涵、原因、挑战、策略和建议为主线，深入思考了研究科技情报安全对于国家科技创新、国际竞争综合较量和国家安全的重要性；鉴别了科技情报安全的本质内涵--信息泄露、成果破坏和定向误导，为识别科技情报的安全威胁提供参考思维逻辑。同时，客观分析了导致科技情报信息安全事件的可能原因，以及保护科技情报安全对应的挑战，提出了科技情报安全保护的策略和具体建议，为我国科技情报安全保护工作的开展贡献了提供了思路。

科技情报安全是一项体系化的工作，涉及我国开展自主知识产权的科技创新工作的每个环节和参与者。本文通过抛砖引玉的方式，为我国科技创新的信息安全贡献了绵薄之力，但是对于国家科技创新保护和情报安全工作而言，仍需要广大科技创新工作者勠力同心，共同关注国家科技创新安全保护问题，贡献智慧，共同守护国家科技战略安全。

参考文献

[1].陈树,李辉,西桂权,谭晓.中美科技竞争视阈下加强国家科技情报体系建设研究[J/OL].情报理论与实践:1-10[2022-10-19].http://kns.cnki.net/kcms/detail/11.1762.G3.20220812.1138.002.html.

[2].陈美华, 王延飞.面向国家科技竞争战略的情报赋能研究——以应对美国涉华科技竞争战略为例[J]. 图书情报知识,2022,39(2):73-82.

[3].郭建伟, 张子成, 燕娜, 等. 科技情报资源与信息安全[J]. 2017 年北京科学技术情报学会年会--“科技情报发展助力科技创新中心建设” 论坛论文集, 2017.

[4].苏凯.从“棱镜门”事件分析信息安全对国家安全的影响及对策[J].网络安全技术与应用,2022(10):162-164.

[5].张一,王亚男,王贵平.社会科学视角下我国网络安全研究的脉络、热点与趋势分析[J].图书情报研究,2022,15(03):98-105.

[6].360 安全大脑—APT 威胁情报中心.披露美国中央情报局 CIA 攻击组织（APT-C-39）对中国关键领域长达十一年的网络渗透攻击[OL].2020-03-03. https://www.360.cn/n/11563.html.

[7].田志宏. APT 组织情报研究年鉴[R].绿盟科技.2022.1-202. http://blog.nsfocus.net/wp-content/uploads/2022/01/APT.pdf.

[8].罗娇,刘细文.知识产权视角下科学数据安全管理的策略选择[J].图书情报工作,2021,65(12):38-46.DOI:10.13266/j.issn.0252-3116.2021.12.003.

[9].张涛,马海群.智能情报分析中数据与算法风险识别模型构建研究[J].情报学报,2022,41(08):832-844.

[10]. 郭鹏.从网络勒索病毒事件分析科技领域安全对国家安全的影响及对策[J].网络安全技术与应用,2022(08):157-159.

[11]. Lesné S, Koh M T, Kotilinek L, et al. A specific amyloid-β protein assembly in the brain impairs memory[J]. Nature, 2006, 440(7082): 352-357.

[12]. Piller C. Blots on a field?[J]. Science (New York, NY), 2022, 377(6604): 358-363.
[13]. 姚斌.高校科研泄密警示录[J].保密工作,2015(02):13-15.DOI:10.19407/j.cnki.cn11-2785/d.2015.02.007.
[14]. Serpanos D, Komninos T. The Cyberwarfare in Ukraine[J]. Computer, 2022, 55(7): 88-91.
[15]. 曾建勋.“十四五”期间我国科技情报事业的发展思考[J].情报理论与实践,2021,44(01):1-7.DOI:10.16353/j.cnki.1000-7490.2021.01.001.
[16]. 曾建勋.基于高端交流平台的科技情报事业发展思考[J].中国图书馆学报,2022,48(03):15-24.DOI:10.13530/j.cnki.jlis.2022021.
[17]. 杨国立.国家战略背景下情报学发展探析[J].情报学报,2022,41(07):762-773.
[18]. 李品.开放科学环境下科技安全的情报保障研究[J/OL].情报理论与实践:1-10[2022-10-23].http://kns.cnki.net/kcms/detail/11.1762.g3.20220705.1016.002.html
[19]. 完颜邓邓, 陶成煦. 美国政府数据分类分级管理的实践及启示[J]. 情报理论与实践, 2020, 43(12): 172-177.
[20]. 王继业,高灵超,董爱强,郭少勇,陈晖,魏欣.基于区块链的数据安全共享网络体系研究[J].计算机研究与发展,2017,54(04):742-749.
[21]. 孙玉欣.基于抗合谋数字指纹的数据库泄密溯源研究[D].南京邮电大学,2021.DOI:10.27251/d.cnki.gnjdc.2021.001510.
[22]. 邱晓慧,杨波,赵孟晨,胡师阳,孙璞.联邦学习安全防御与隐私保护技术研究[J/OL].计算机应用研究:1-13[2022-10-17].DOI:10.19734/j.issn.1001-3695.2022.03.0164.
[23]. 胡成,朱雪忠,代志在.国家知识产权安全情报体系构建研究[J].情报杂志,2022,41(02):35-42+34.

作者贡献说明

:收集梳理资料，撰写论文初稿，论文修改；
:确定论文选题，提出论文框架，设计主体内容，指导论文修改。

Thinking on Information Security in Scientific &Technological Intelligence

Abstract: [Purpose/significance] The scientific and technological information created by scientific and technological innovation is an important achievement of national scientific & technological innovation activities. The information security of scientific & technological intelligence profoundly impacts our scientific & technological innovations, industrial advancements and even national security. Researching the information security of scientific & technological intelligence is helping to discover security threats of our scientific & technological innovations and to develop effective measures for avoiding information security events. Meanwhile, building an information security protection system oriented to scientific & technological innovations is essential to protect the security of innovations. **[Method/process]** This paper first analyzes the security information essential connotation of scientific & technological innovation, then concludes the information security issues of scientific & technological innovations, and finally excavates the existing reasons causing information security problems. From the security protection perspective of scientific & technological innovation, this work proposes

corresponding suggestions for protecting scientific & technological innovations and explores the solutions to tackle the information security issues in scientific & technological innovation.

[Result/conclusion] The information security issues of scientific & technological intelligence are summarized as information leakages, data destructions and misleading by false research. Protecting information security of scientific & technological intelligence is up against many challenges, such as difficulty in perception, prevention, monitoring, obtaining evidence, discriminating, and coping. The information security recommendations for protecting scientific & technological intelligence are carried out simultaneously from five levels: classification and grading of scientific & technological intelligence, facility protection, data protection, authority protection and applications of information security technologies. Meanwhile, solutions, including strengthening the awareness of scientific & technological intelligence protection of scientific researchers, increasing the monitoring of cyber-attacks, and promoting digital fingerprint technology applications to scientific & technological intelligence, are crucial to protecting the security of national technological innovations.

Keywords: Scientific & Technological Innovations; Information Security; Security of Scientific & Technological Intelligence.

Affiliation: 1. Library of South China Normal University, Guangzhou China, 510631